SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Group Law on Elliptic C

av

Jelena Petkovic

2019 - No K22

Group Law on Elliptic C

Jelena Petkovic

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sofia Tirabassi

2019

Contents

1 Introduction

In this thesis we will go through elliptic curves, not to be confused with ellipses, which are defined as plane algebraic curves with an equation of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

It is possible to define a binary operation on the set of points of an elliptic curve. We will do it in the field of real numbers. This turns out to be associative, having an identity element. In addition each point in the elliptic curve has an inverse with respect to this operation. Thus the set of points of an elliptic curve can be given a group structure. We will also see that the operations do not depend on the order of the points, so we will get an abelian group.

The goal of this thesis is to introduce group law on elliptic curves. In order to do so, the reader will be provided with the ideas and theorems behind elliptic curves and how to apply the group law. For this we will study algebraic curves in the affine plane and eventually move to the projective plane. We will also show some examples for how to calculate and use what is provided in this paper. We will first start by introducing commutative algebra which is fundamental in studying elliptic curves, and this will be brought up again in section 6.

Secondly, we will bring up a major tool in terms of studying algebraic curves in the third section, namely homogeneous coordinates, where we will leave the typical notion of parallel lines and study how algebraic curves behave at infinity.

In the fourth section we will bring up the idea that a curve may intersect multiple times at a point, where we will introduce properties for the reader to use for counting multiplicities between another curve or a line.

We will also characterize tangent lines which will be used when working with elliptic curves. And lastly, we will provide the reader enough information to work with group laws for elliptic curves where the reader will be able to understand how to compute a line through said elliptic curve and know what the points of intersection represent.

2 Commutative Algebra

To begin with, this section only serves the purpose of introducing preliminary notions which will be used later. The reader has probably previously encountered the notion of a field, where a set of operations are defined, and is aware that a field is a fundamental algebraic structure. Thus, the definition of a field will not be brought up.

As mentioned in the introduction, elliptic curves have a group structure which satisfies *commutativity*. Therefore, we need to introduce the notion of commutative algebra which will be used later in the text.

Definition 2.1. A K-algebra, is a commutative ring A together with a ring homomorphism $\phi : K \to A$ where we can define an operation

$$K \times A \to A \qquad (\lambda, a) \mapsto \lambda a$$

by setting $\lambda a := \phi(\lambda) \cdot a$, it fulfills

$$\lambda(a \cdot b) = \phi(\lambda) \cdot (a \cdot b) = (\phi(\lambda) \cdot a) \cdot b = a \cdot (\phi(\lambda) \cdot b)$$

$$\lambda(a+b) = \phi(\lambda)\cdot(a+b) = \phi(\lambda)\cdot a + \phi(\lambda)\cdot b$$
$$\Rightarrow \lambda a + \lambda b$$

for any $a, b \in A$, $\lambda \in K$. Thus A has a K-vector space structure which is in some sense compatible with the ring structure.

Since K-algebra S is in particular a vector space, it would make sense to consider the dimension which we denote by $\dim_K S$.

Example 2.2. If we have $K[x_1, ..., x_n]$, which denotes the ring of polynomials in the variables $x_1, ..., x_n$ over K, and I is our prime ideal. Then with the ring homomorphism we would have

$$\phi : K \to K[x_1, ..., x_n]/I$$
$$\lambda \mapsto \lambda + I$$

that gives a K-algebra structure on
$$K[x_1, ..., x_n]/I.$$

Note that
$$\lambda(f + I) = \lambda f + I$$

3 Affine and Projective Plane Curves

This section is going to cover the affine and projective plane as well as curves in respective plane. Some basic information about each plane will be introduced in order to know the differences between the planes and why we are working with two different planes.

We will start with the affine plane. As mentioned in [4], the affine plane is a system of points and lines that satisfy:

1. Each line has at least two points
2. Given any line and any point not on that line there is a unique line which contains the point and does not meet the given line
3. There exists three non-collinear points (points not on a single line)

We will denote $\mathbb{A}^2(K) := K^2$ as the affine plane over the field K, and $K[X, Y]$ the polynomial algebra in the variables X and Y over K.

Definition 3.1. A subset $\Gamma \subset \mathrm{A}^2(K)$ is called an affine irreducible curve if there exists a non-constant irreducible polynomial $f \in K[X, Y]$ such that $\Gamma = Z(f)$. Where

$$Z(f) := \{(x, y) \in \mathbb{A}^2(K) \mid f(x, y) = 0\}$$

is the *zero set of f*, see [1]. We write $\Gamma : f = 0$ for this curve and call $f = 0$ an equation for Γ.

Given Γ a plane algebraic curve we get an irreducible polynomial f and so a prime ideal $I = (f)$. The quotient $K[X, Y]/I$ is denoted by $K[f]$ and it is called the affine coordinate ring of Γ. Note that this is a domain as I is prime. So we can consider the field of quotient $K[X, Y]/I$ which we will denote by $K(\Gamma)$ and we will call this the field of rational functions of Γ. Note that the elements of $K(\Gamma)$ can be represented as

$$h \quad \text{such that} \quad \frac{f+I}{g+I} \Big/ g \notin I.$$

Remark 3.2. A field K is called algebraically closed if every non-constant polynomial $f \in K[x]$ in one variable has a zero [2]. In addition, any algebraically closed field is necessarily infinite: If $K = \{c_1, ..., c_n\}$ was finite, the polynomial $f = \Pi_{i=1}^{n}(x - c_i) + 1$ would have no zero.

Example 3.3. The field of real numbers, $\mathbb{R}$, is not algebraically closed because the polynomial equation $x^2 + 1 = 0$ has no solution in real numbers.

A polynomial in two variables is a finite sum of terms of the form ex^iy^j, where the coefficient e is in the field K and the exponents i and j are non-negative integers. So we can write

$$f(x, y) = \sum ex^iy^j$$

which is the *degree* of a monomial and the the *degree of* f is the maximum degree of terms appearing in the expression of f.

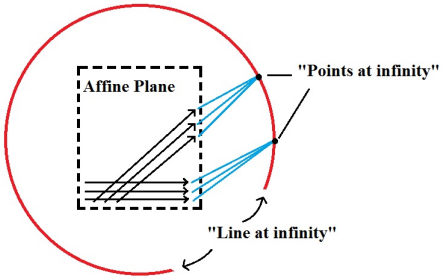
Example 3.4. Consider the polynomial:

$$y^3 = 5x^4 + 3x^3 - 13x^2 + 6$$

and the following terms will have the degrees: $3, 4, 3, 2, 0$. The zero sets of polynomials with maximum degree 3 are called cubics.

For us to move from the affine plane to the projective plane we have to add *points at infinity*. We can add these points by taking a family of parallel lines and agree that they meet at a new point at infinity. Hence, we are leaving the notion that parallel lines never intersect, which is fundamental in the affine plane. Abandoning the notion will ensure us that any two lines, even if parallel, will meet at a point, and allowing us to augment the plane at the horizon which we are able to do by adding points at infinity.

A different family of parallel lines will meet at another point at infinity, resulting in for every family of parallel lines there exists a point at infinity. The collection of new points that go against infinity is declared to be a new line, called the *line at infinity*.



The line at infinity will be the augmentation from the affine plane to the projective plane where we then can study elliptic curves.

The *projective plane*, $\mathbb{P}^2$, over a field K is the set of lines in K^3 through the origin determined by ordered triplets (x_0, x_1, x_2), where the triplets are not all zero, as explained in [1]. The points $P \in \mathbb{P}^2(K)$ will be given by triplets (tx_0, tx_1, tx_2), where the term t varies over all nonzero numbers and indicates that all triplets represents the same point.

Example 3.5. The point $P = t(1, -2, 3)$ in $\mathbb{P}^2$ over $\mathbb{R}$ can be represented as

$$2(1, -2, 3) = (2, -4, 6)$$

$$-3(1, -2, 3) = (-3, 6, -9)$$

$$\frac{1}{3}(1, -2, 3) = (\frac{1}{3}, \frac{-2}{3}, 1)$$

Showing that they all represent the same point as t varies over real numbers.

So for every $t \neq 0$ the expression (tx_0, tx_1, tx_2) is a set of *homogeneous coordinates* for the point $P = t(x_0, x_1, x_2)$ according to [1], which allows us to study curves at infinity.

In addition, since we are working with homogeneous coordinates it makes sense to introduce *homogeneous polynomials* as well.

Definition 3.6. Let F be a homogeneous polynomial of degree d, we will have

$$F(\lambda x_0, \lambda x_1, \lambda x_2) = \lambda^d F(x_0, x_1, x_2)$$

for any $\lambda \in K$.

To simplify, a homogeneous polynomial is a polynomial where every term is of the same degree.

Let $K[X_0, X_1, X_2]$ be the polynomial algebra over K. If $F \in K[X_0, X_1, X_2]$ is a homogeneous polynomial and $P = (x_0, x_1, x_2)$ is point of $\mathbb{P}^2(K)$, we will call P a zero of F if $F(x_0, x_1, x_2) = 0$. In addition, if the degree $F = d$, we will have $F(tx_0, tx_1, tx_2) = t^d F(x_0, x_1, x_2)$ for any $t \in K$, and therefore the condition $F(x_0, x_1, x_2) = 0$ does not depend on the particular choice of homogeneous coordinates for P, as mentioned in [4]. Thus we can write $F(P) = 0$. The set

$$Z_+(F) := \{P \in \mathbb{P}^2 \mid F(P) = 0\}$$

will be called the zero set of F in $\mathbb{P}^2$.

Definition 3.7. A subset $\Gamma \subset \mathbb{P}^2$ is called a *plane projective algebraic curve* if there exists a non-zero homogenous polynomial $F \in K[x_0, x_1, x_2]$ where the degree of the polynomial $F > 0$ such that $\Gamma = Z_+(F)$.

Example 3.8. Curves of degree 1 in $\mathbb{P}^2(K)$ are called projective lines. They are solution sets of homogeneous linear equations that satisfy

$$a_0x_0 + a_1x_1 + a_2x_2 = 0 \qquad (a_0, a_1, a_2) \neq (0, 0, 0).$$

As stated in Kunz [4], two projective lines will always intersect, and the intersection will consist of one point if and only if the lines are different. Where the system of equations

$$a_0X_0 + a_1X_1 + a_2X_2 = 0, \quad b_0X_0 + b_1X_1 + b_2X_2 = 0$$

has exactly one non-trivial solution (x_0, x_1, x_2) that is unique up to a constant factor if and only if the coefficient matrix of the systems

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix}$$

has rank 2, the dimension of the vector space generated by its columns. Otherwise the intersection will be the whole line.

The passage, [4], from affine to projective plane is given by the injection

$$i : \mathbb{A}^2(K) \to \mathbb{P}^2(K)$$

$$(x_1, x_2) \mapsto (1, x_1, x_2)$$

where the coordinates preserve their distinctness. We identify $\mathbb{A}^2(K)$ by its image under i, and then $\mathbb{A}^2(K)$ will be the complement of the line $X_0 = 0$ in $\mathbb{P}^2$. This line will be called the line at infinity of $\mathbb{P}^2$, and its point will naturally be called the points at infinity.

If given a nonzero polynomial $f(x_1, x_2)$ of degree d and extend the curve $f(x_1, x_2) = 0$ from the affine plane to the projective plane. The homogenization given by the injection $F(x_0, x_1, x_2)$ of f is the homogeneous polynomial obtained after multiplying each term of f by the power of x_0 needed to produce a term of degree d, as [1] describes. That is, if

$$f(x_1, x_2) = \Sigma e_{ij} x_1^i x_2^j$$

we get the *homogenization*

$$F(x_0, x_1, x_2) = \Sigma e_{ij} x_1^i x_2^j x_0^{d-i-j}.$$

Resulting in $F = 0$ and $f = 0$ containing the same points of the affine plane. Therefore we call $F = 0$ the extension, or homogenization, of the curve $f = 0$ to the projective plane. Consequently, the *dehomogenization* is when we move from the projective plane back to the affine plane where we set $x_0 = 1$ to receive the affine curve.

Example 3.9. If we have the curve in $\mathbb{R}^2$

$$x^4 + 3x^2y - 4y^4 + 5y^3 + y^2 - 2y - 6 = 0$$

which is our curve $f(x, y) = 0$, and each term has respective degree: $4, 3, 4, 3, 2, 1, 0$. The coordinate transformation which maps the curve from $\mathbb{A}^2(K) \to \mathbb{P}^2(K)$ will be the homogenization $f(x, y) = 0 \to F(x_0, x_1, x_2) = 0$, where $x = x_1$, $y = x_2$ and $z = x_0$

$$x_1^4 + 3x_0x_1^2x_2 - 4x_2^4 - 5x_0x_2^3 - x_0^2x_2^2 - 2x_2x_0^3 + 6x_0^4 = 0.$$

Our point at infinity is when $\{[0, x_1, x_2]/F(0, x_1, x_2) = 0\}$, which we receive after we plug in $x_0 = 0$. We will then have

$$x_1^4 - 4x_2^4 = 0$$

$$x_1^4 = 4x_2^4$$

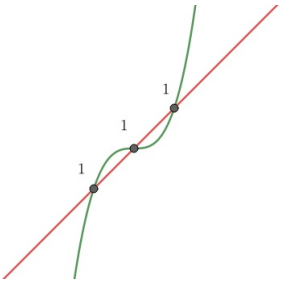
To find the point at infinity we only need to utilize simple math

$$x_1 = \sqrt{2x_2}$$

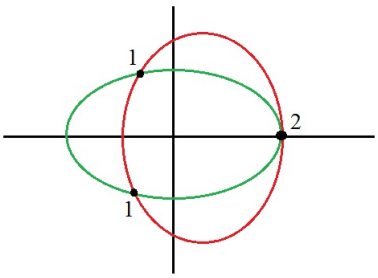
and if $x_2 \neq 0$ our points at infinity will be $[0, \pm\sqrt{2x_2}, x_2]$, and if we set $x_2 = 1$, our points are $= [0, \pm\sqrt{2}, 1]$.

4 Intersection of Curves

This section will go through intersections of curves. The reader has probably previously encountered a curve which intersects another curve or a line more than once (see figure below) and is somewhat familiar with intersection. We will now turn to the idea that two curves can intersect more than once at a point.



If a curve intersects with another curve or a line at a given point, we can assign a *multiplicity*. We can then count the number of times they intersect at the point of intersection with some properties, leaving the idea that they will only intersect once at a point.



We recall that a ring is local if it has only one maximal ideal. If given a point $P \in \mathbb{A}^2$ we define the local ring as

$$\mathcal{O}_P := \{\frac{f}{g} : f, g \in K[X, Y] \text{ with } g(P) \neq 0\} \subset K(X, Y)$$

As mentioned in [2], the local ring $\mathcal{O}_P$ will take on a well-defined ring homomorphism

$$\mathcal{O}_P \to K, \ \frac{f}{g} \mapsto \frac{f(P)}{g(P)}.$$

To show well-definedness, we note that

$$\frac{f}{g} = \frac{f'}{g'} \Leftrightarrow fg' - f'g = 0$$

.

We want to show that $\frac{f(P)}{g(P)} = \frac{f'(P)}{g'(P)}$. If we were to plug in a point P in the expression above and rearrange, we will have

$$\frac{f(P)}{g(P)} - \frac{f'(P)}{g'(P)} \Rightarrow \frac{fg'(P) - f'g(P)}{g(P)g'(P)} = 0$$

So we can reach a conclusion and observe that $\mathcal{O}_P$ is indeed a local ring. In fact

$$\mathfrak{m}_P := \{\frac{f}{g} \mid f(P) = 0\}$$

is a maximal ideal. If q was another maximal ideal and let $f \in q$ such that $f \notin \mathfrak{m}_P$. This exists because otherwise $\mathfrak{m}_P \subseteq q$ where $\mathfrak{m}_P$ is no longer the maxima. Now note that f is invertible.

Ideals contains an invertible, elements such that $u^{-1} \cdot u = 1$ for every element in the ideal. In our case, if $f = \frac{h}{g}$ where $h(P) \neq 0$ and $g(P) \neq 0$ we would have the inverse $f^{-1} = \frac{g}{h}$. So q is our whole ring and is not the maximal ideal.

Definition 4.1. Let $f, g \in K[X, Y]$ and let $P \in \mathbb{A}^2$. The intersection multiplicity of f, g at P is $I_P(f, g) = \dim_K \mathcal{O}_{\mathbb{A}^2,P}/\left(\frac{f}{1}, \frac{g}{1}\right)$. If C and D are curves in $\mathbb{A}^2$, then let $I(C) = (f)$ and $I(D) = (g)$, and the intersection multiplicity of C and D at P is $I_P(C, D) = I_P(f, g)$.

Let P be O that denotes the origin $(0, 0)$ and assign a value $I_P(f, g)$ to every pair of polynomials f and g. This value is called the *intersection multiplicity* of f and g at P, in our case O, and we want to count the intersection multiplicity at the origin since the algebra is easiest there. We may think of the intersection multiplicity as the number of times our curves f and g intersect at the origin.

We have defined the intersection multiplicity as $I_P(f, g) = \dim_K \mathcal{O}_{\mathbb{A}^2,P}/(f, g)$ where (f, g) is the ideal generated by the polynomials f and g in the local ring. Then for a point P on the curve f in the affine space $\mathbb{A}^2$, one can think according to [4] of the ring being attached to the curve at the point P. If we want the intersection multiplicity at point $P = (p_1, p_2)$ the maximal ideal will be $\mathfrak{m}_P = (x_1 - p_1, x_2 - p_2)$ and we will define intersection multiplicity as

$$I_P(f, g) := \dim_K \mathcal{O}_{\mathbb{A}^2,P}/\left(\frac{f}{1}, \frac{g}{1}\right)\mathfrak{m}_P$$

In terms of counting the value for intersection multiplicity we have certain properties to utilize. Through out the properties, P will be the origin.

Lemma 4.2. *$I_P(f, g)$ is a non-negative integer if f, g define different curves.*

The proof will not be shown since it is out of this paper, but is proven in [4] with Theorem 1.4 found on page 16. However, an short summary will be provided.

Since we are dealing with irreducible curves we will have that f, g are irreducible. If $f = \lambda g$ for some $\lambda \in K$ we will have an infinite amount of solutions because they share a common factor, and thus every point will lie within another curve. One may think of f and g as two distinct lines, but if g is multiplied with λ, the two lines will over lap, resulting in having the same solution no matter what is plugged in. Otherwise, f and g will have no common factor and have a finite solution.

Property 4.3. $I_P(f,g) = I_P(g,f)$

Proof. Because f and g are generated by the same ideal we have

$$\Big(\frac{f}{1},\frac{g}{1}\Big) = \Big(\frac{g}{1},\frac{f}{1}\Big).$$

Since the curves will also be generated by the same ideal in the local ring, we will have that

$$\mathcal{O}_P/(\frac{f}{1},\frac{g}{1}\Big) = \mathcal{O}_P/(\frac{g}{1},\frac{f}{1}\Big)$$

proving that the intersection multiplicity is symmetrical. □

Property 4.4. $I_P(f,g) \geq 1$ *if and only if f and g both contain the origin.*

Proof. First we will show that if $0 \notin f$ and $0 \notin g$ we will have $I_P(f,g) = 0$. We have a field $K = K[X,Y]/(f)$ and a ring $\mathcal{O}_P = Q\Big(K[X,Y]/(f)\Big)$ where the field is contained in the ring, thus we will have the following maps

$$\phi_1 : K \to K[X,Y] \qquad a \mapsto a$$

$$\phi_2 : K[X,Y] \to K[X,Y]/(f) \qquad g \mapsto g + (f)$$

$$\phi_3 : K[X,Y]/(f) \to Q\Big(K[X,Y]/(f)\Big) \qquad g + (f) \mapsto \frac{g+(f)}{1+(f)}$$

Adding the maps together, we will get an injective map

$$\phi_1 \cdot \phi_2 \cdot \phi_3 : K \hookrightarrow \mathcal{O}_P$$

$$a \mapsto \frac{a+(f)}{1+(f)} \to \frac{a(P)}{1(P)} = a$$

where $1 \to \frac{1+(f)}{1+(f)}$ is the identity element different from zero. The added maps give a ring morphism that is different from zero where it either takes on every element or none. Therefore resulting in our field K having the kernel $\phi = (0)$ and we will have that $I_P(f,g) = 0$ because the kernel is zero.

Hence we may assume that if $f(P) = g(P) = 0$ where they do contain the origin, and as the opposite of the above paragraph, we will have that the intersection multiplicity is greater or equal to one, since they can intersect once or more at the point because the kernel will be different from zero. □

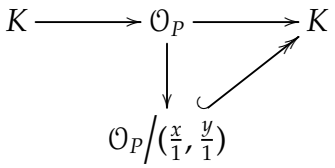
In addition, it only makes sense that if two curves do not contain the same point they will not intersect because they have nothing in common at the point.

Property 4.5. $I_P(x,y) = 1$

Proof. Using the proof from property 4.4 and if we assume that $f(P) = g(P) = 0$ as well as defining the maximal ideal as

$$\mathfrak{m} := (\frac{x}{1}, \frac{y}{1})$$

we will have the following



Because of the first map, as in the proof in property 4.4, we will get

$$a \mapsto a + (f).$$

However, since we have the maximal ideal as an element the ring will take on the form

$$\mathcal{O}_P/\Big(\frac{x}{1}, \frac{y}{1}\Big)$$

which is a field. Since it is a field we will get that the first map gives us

$$a \mapsto a + (f)$$

where $f(P) = 0$ because if the maximal ideal and thus the last mapping will only have the element contained in the field and the sequence has the following form

$$a \mapsto a + f(P) \mapsto a.$$

To conclude, the sequence will map the element back to itself, resulting in that we can only have one solution that equals to one. Thus, the property is proven. □

We recall that the factors of two numbers are called co-prime when they only have one as their common factor.

Property 4.6. *$I_P(f, g) = I_P(f, g + fh)$ if and only if f, g, h are nonzero polynomials that do not vanish at P.*

Proof. Let P be a point in $\mathbb{A}^2$ and let $f, g, h \in K[X, Y]$ such that f and g are co-prime and such that fh and g have the same degree and do not vanish at P. We will then have that

$$(f, g + fh) = \Big(\frac{f}{g}, \frac{g}{g} + \frac{f \cdot h}{g}\Big) = (f, g)$$

Thus the property will hold, as mentioned in [3] (Lemma 2.11, p 13). □

Property 4.7. *$I_P(f, gh) = I_P(f, g) + I_P(f, h)$ where f, g, h are any three irreducible polynomials. Where they are not multiples, no common factor containing P, and g is nonzero.*

Before proving the property, we have to first introduce an exact sequence and the following lemma. An exact sequence is a sequence of objects and homomorphisms, that is either finite or infinite, so that the image of one of the homomorphisms equals the kernel of the next.

Lemma 4.8. *Let A be a ring and let $u, t \in A$ be two of its elements so it maps $u\cdot, t\cdot : A \to A$ given by $x \mapsto ux$ and $x \mapsto tx$ respectively are injective. Then we will have that $t\cdot$ induces a morphism $A/(u) \to A/(ut)$ and the sequence*

$$0 \to A/(u) \xrightarrow{t\cdot} A/(ut) \xrightarrow{q} A/(t) \to 0$$

is exact, where q is the natural quotient map.

Proof. Using the proof in [3], let A be as in the statement, and $u, t \in A$ be two of its elements. We can define the map $A \times A \to A$ given by $(y, x) \mapsto yx$. Since $(u), (ut)$ and (t) are ideal of A, we can construct the rings $A/(u), A/(ut)$ and $A/(t)$ respectively (note that these are also K-algebras). Let ψ and ϕ be the two maps induced by $t\cdot$ and the natural quotient map q respectively. Hence,

$$\psi : A/(u) \to A/(ut) \quad \phi : A/(ut) \to A/(t)$$

and

$$x + (u) \mapsto tx + (ut) \quad x + (ut) \mapsto x + (t).$$

Where we have:

1. The map ψ is injective. Let $x + (u) \in \ker \psi$, we will then have that $\psi(x + (u)) = 0 + (ut)$ according to the lemma. Then $tx \in (ut)$ where there exists $s \in A$ such that $tx = s \cdot t \cdot u$, and after rearranging we will have that $t(x - su) = 0$, but $t \neq 0$ or else the map would not uphold. Thus, we must have that $x - su = 0$ which implies $x = su$, where $x \in (u)$ and therefore $x + (u) = 0$, which means that the Ker $\psi = 0$ and the map is injective.

2. Because q is the natural quotient map, ϕ is surjective.

3. If we let $y \in A$, then $y + (ut)$ is the image of ψ and $y + (ut)0tx + (ut)$ for some $x \in A$. Thus $\phi(tx + (ut)) = tx + (t) = 0$. Because $tx \in (t)$ we will have that the Im $\psi \subseteq$ Kerϕ. Therefore, $y + (ut) \in \ker \phi$ where $\phi(y + (ut)) = y + (t)y \in (t)y = tx$ for some $x \in K[X, Y]$. Therefore $(ut) = tx + (ut) = \psi(x + (u))$, that the image of ψ is equal to the kernel of ϕ.

□

From the listing of 1, 2 and 3, we can conclude that the sequence we have is exact. We can then use lemma 4.8 to prove our property.

Proof. Proof of property. To prove the property we apply the lemma above but with different identifications. We will have that our $A = \mathcal{O}_P/(f)$ and our elements are $u = g + (f)$ and $t = h + (f)$. This would give us

$$\Big(\mathcal{O}_P/(f)\Big)\Big/(g) = \mathcal{O}_P/(f, g)$$

where this is $A/(u)$ in the lemma.

$$\Big(\mathcal{O}_P/(f)\Big)\Big/(h) = \mathcal{O}_P/(f, h)$$

where this is $A/(t)$ in the lemma.

$$\Big(\mathcal{O}_P/(f)\Big)\Big/(gh) = \mathcal{O}_P/(f, gh)$$

where this is $A/(ut)$ in the lemma.

The lemma implies that the sequence with our identifications

$$0 \to \mathcal{O}_P/(f,g) \to \mathcal{O}_P/(f,gh) \to \mathcal{O}_P/(f,h) \to 0$$

is exact. Where we have the dimension property

$$\dim \mathcal{O}_P/(f,h) + \dim \mathcal{O}_P/(f,g) = \dim \mathcal{O}_P/(f,gh).$$

This allows us to separate the terms and still have the same result when counting intersection multiplicity. □

When computing intersection multiplicity at the origin one can disregard factors that do not contain the origin, which will be useful later on.

Corollary 4.9. *If f, g, and h are curves and $h(P) \neq 0$, we have*

$$I_P(f,gh) = I_O(f,g)$$

Proof. The properties from before, 4.7, 4.4 and 4.2 shows

$$I_P(f,gh) = I_O(f,g) + I_O(f,h) = I_O(f,g)$$

Where $I_P(f,h) = 0$ because h does not contain the origin. □

Example 4.10. We will use the properties to compute the intersection multiplicity between the curves $y^4 = x^3$ and $x^2y^3 = y^2 - 2x^7$ at the origin. First, we start by putting the curves in the same form as the properties and change P to O:

$$I_O(y^4 - x^3, 2x^7 + x^2y^3 - y^2)$$

By first using property 4.7 the intersection multiplicity will be the following:

$$I_O(y^4 - x^3, 2x^7 + x^2y^3 - y^2 + 2x^4(y^4 - x^3)) =$$
$$I_O(y^4 - x^3, 2x^4y^4 + x^2y^3 - y^2)$$

Then using property 4.7:

$$I_O(y^4 - x^3, y^2(2x^4y^2 + x^2y - 1)) =$$
$$I_O(y^4 - x^3, y^2) + I_0(y^4 - x^3, 2x^4y^2 + x^2y - 1)$$

Since $I_O(f,h)$ does not contain the origin one can utilize corollary 4.9 that gives the outcome:

$$I_O(y^4 - x^3, y^2)$$

Here property 4.6 can be used when computing:

$$I_O(y^4 - x^3 - y^2(y^2), y^2)$$
$$\Rightarrow I_O(-x^3, y^2)$$

As a result of property 4.5 and 4.7 the final outcome will be:

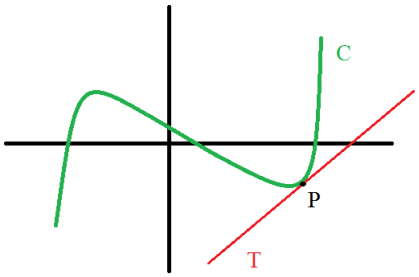
$$2I_O(-x^3, y) =$$
$$6I_O(y, -x) = 6 \cdot 1 = 6$$

Therefore the intersection multiplicity of the two curves is 6 at the origin.

As mentioned in [1], there exists a transformation map (theorem 3.4) which is out of this thesis paper, that *fixes* points if the points are mapped to themselves. This transformation map fixes points from the affine plane to the projective plane and preserves multiplicity. Since it preserves multiplicity as well as fixing the same points in the affine plane to the projective plane, we can utilize the same properties of intersection multiplicity in the projective plane.

5 Tangent and Points

From this section on we will only work in $\mathbb{R}$, that is $K = \mathbb{R}$.The *tangent line* is explained the easiest as the line to a curve at a given point as the straight line that just touches the curve at the given point with the same slope, same direction at point of contact. A tangent line is also the unique line that intersects a curve C at point P more than once.



Definition 5.1. For a curve F in $\mathbb{P}^2(\mathbb{R})$ and a point $P \in \mathbb{P}^2(\mathbb{R})$ we call

$$m_P(F) := min\{\, I_P(F, l) \mid l \text{ a line through } P\}$$

the multiplicity of P on F, as defined in [4]. By property 4.4 it is clear that $m_P(F) = 0$ if and only if $P \notin Z(F)$. Because there will always be a line l through P that is not a component of F, we will have $I_P(F, l) < \infty$ and thus $m_P(F) < \infty$.

Definition 5.2. Let $P \in Z(F)$ and let L be a line through P. Kunz says, if $I_P(F, l) > m_P(F)$, we call l a tangent to F at P.

In other words, a straight line is said to be a tangent to a curve if it intersects the curve at a point P more than once.

In addition, the tangent line passes through a point where it meets a curve, called the *point of tangency*, where the tangent line is viewed to move in the same direction as the curve, and is therefore the best straight-line approximation to the curve at that point.

If we want the tangent line to an affine curve $f(x, y)$ at some point $P = (a, b)$ we want to approximate the function value of the curve as near as possible with the function value of our tangent line. Naturally, this approximation will only be good when x and y are relatively near a and b. The tangent line approximation for a function $f(x, y)$ near (a, b) is called the first degree Taylor polynomial of $f(x, y)$, which has the form

$$T_{a,b}(x, y) := \frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b)$$

where the partial derivatives are the slope of the tangent line at the given point, which makes the tangent line move in the same direction as the curve and allows us to have the best linear approximation.

Depending on what happens when computing the tangent line different points are acquired. As brought up in [5], if both partial derivatives vanish when evaluated at (a, b) the tangent will not be defined at point P, we call such points a *singular point* on the curve.

In other words, a point is singular if

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) = (0, 0).$$

However, if the curve does not contain any singular points, the curve is said to have *non-singular points* or a *smooth* curve

$$\Big(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\Big) \neq (0,0).$$

Where only one, if not both, partial derivatives is not equal to zero.

A flex point is a generalized inflection point, where the curve changes from concave to convex or vice versa. A point is a flex of C such that the curve C is non-singular at P and G intersects the tangent at P at least three times at the given point P.

In other words, C has a flex at P if it has a tangent line l at P where $I_P(l, C) \geq 3$. It is important to know that transformations preserve flexes since they also preserve tangents and intersection multiplicities.

Example 5.3. If we wanted to study whether or not the point P at the intersection between the curve $y^3 = x^3 + 3x$ and its tangent line is a flex at the origin, we would first have to compute the tangent line.

We start by first using the definition of the tangent line to find the line at the origin

$$\frac{\partial f}{\partial x} = 3x^2 + 3.$$

We plug in $x = 0$ and receive an expression for every y

$$\frac{\partial f}{\partial x} = 3$$

We continue the process with

$$\frac{\partial f}{\partial y} = 3y^2.$$

We plug in $y = 0$ and receive an expression for every x

$$\frac{\partial f}{\partial y} = 0.$$

Lastly we put the partial derivatives in the definition and the tangent line will be

$$T_{0,0}(x, y) = 3(x - 0) + 0(y - 0) = 3x.$$

In order to find out if the point is a flex we need to count the intersection multiplicity at the origin

$$I_O(y^3 - x^3 - 3x, 3x)$$

First we use property 4.6 and get the following:

$$I_O(y^3 - x^3 - 3x + (3x), 3x) =$$

$$I_O(y^3 - x^3, 3x)$$

Secondly, we can use property 4.7 that gives us:

$$I_O(y^3 - x^3, 3x) =$$

$$I_O((y^3 - x^3, x) + I_O(y^3 - x^3, 3)$$

Since the last term does not contain the origin we can disregard it according to corollary 4.9. In addition, since the first equation only differs from y by multiples of x we can eliminate the x terms:

$$I_O(y^3, x)$$

Using property 4.3 allows us to change the position of x and y, then lastly use property 4.7

$$3I_O(x, y) = 3$$

showing that the point is a flex.

We can still use the definition of a tangent line in the projective plane since all we need to do to be able to apply the same definition is to choose the right map after we have chosen the point we want to study.

6 Group Laws on Elliptic Curves

The point of an elliptic curve has an abelian group structure, that is when applying group operations to elements they do not depend on the order of which they are written. The goal of this section is to illustrate the group laws on elliptic curves, that are irreducible cubics with respect to a flex at the origin.

Definition 6.1. An *elliptic curve* in $\mathbb{P}^2(\mathbb{R})$ is a smooth curve of degree 3 for which it has a point satisfying the equation

$$y^2 = x(x-1)(x-a) \quad \text{when} \quad a \neq 0, 1. \tag{1}$$

We want to define an abelian group structure as a set of points. We will define a binary operation by + and the identity element denoted as O. In order to analyze points on an elliptic curve, which is received by intersecting lines or other curves with C, we need further theorems.

Theorem 6.2. *Let l be a line that intersects an irreducible cubic C at least twice, counting multiplicities. Then l intersects C exactly three times, counting multiplicity.*

Proof. If we take a general line and a general curve

$$L : \alpha x + \beta y + \gamma = 0$$

$$C : y^2 - x^3 - ax^2 - bx - c = 0$$

and set that $\alpha \neq 0$, we will have the following expression for x:

$$x = \frac{-\beta y + \gamma}{\alpha}.$$

If we then plug in the expression for x in the curve where $\beta \neq 0$ we will have

$$y^2 - \Big(\frac{-\beta y - \gamma}{\alpha}\Big)^3 - a\Big(\frac{-\beta y - \gamma}{\alpha}\Big)^2 - b\Big(\frac{-\beta y - \gamma}{\alpha}\Big) - c = 0 \tag{2}$$

which is a polynomial of degree three, where the leading factor would be y^3, with two roots y_1, y_2. Since we have two roots it will split completely and because the leading factor is y^3 we will have a third root y_3.

If we instead have that $\beta = 0$, our polynomial would be

$$y^2 - \left(\frac{-\gamma}{\alpha}\right)^3 - a\left(\frac{-\gamma}{\alpha}\right)^2 - b\left(\frac{-\gamma}{\alpha}\right) - c = 0 \tag{3}$$

which is a polynomial of degree two where it seems that a point missing. We can observe that the point at infinity is $(0, 1, 0)$, which is in the intersection between the line and the curve. Thus we will have a point $P_i = (x_i, y_i)$ in every intersection, making the point at infinity our third root.

If $\alpha = 0$, we will have $y = \frac{-\gamma}{\beta}$, and if we plug in the expression in our curve we will receive a polynomial of degree three similar to (6)

$$\left(\frac{-\gamma}{\beta}\right)^2 - x^3 - ax^2 - bx - c = 0 \tag{4}$$

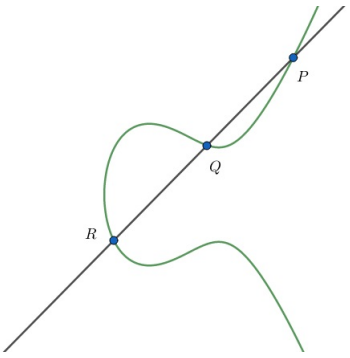
where we will have two roots, x_1, x_2. If we then split the polynomial completely as before, we will get a third root since the leading factor is of degree three. □

The third intersection between the line PQ and C will be the point R such that the line PQ intersect C at the points P, Q, R listed by multiplicity.

Listed by multiplicity means that the point of intersections between the curve C and a line G appears in a list as many times as C and G intersect at the point.

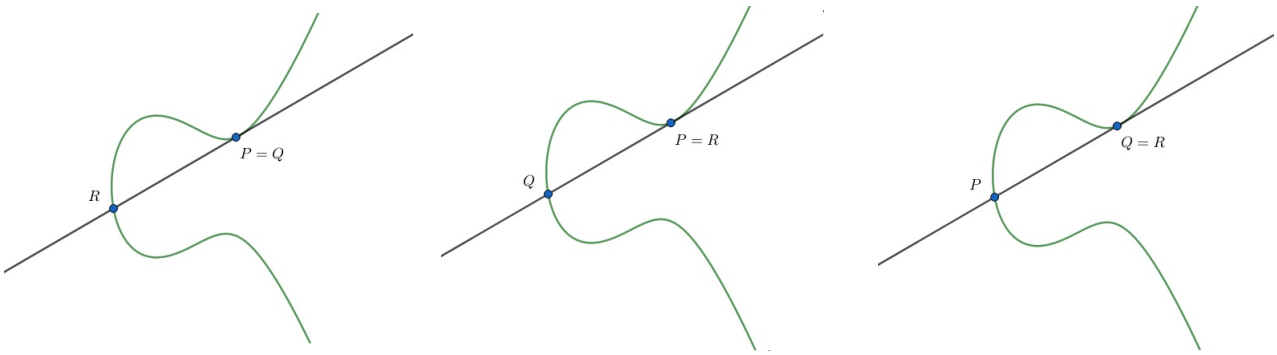
Example 6.3. If the list were P, P, Q, Q, Q, R, R, S for distinct points from P to S. Then C and G intersect two times at P, three times at Q, two times at R and once at S.

Let $E = Z_+(f)$ be an elliptic curve and let $G = Z(ax + by)$ be a line in $\mathbb{P}^2(\mathbb{R})$. By the assumption in theorem 6.2, G should intersect the curve E in three points P, Q, R, where two if not all three of them may coincide. If we first let the the three points be distinct, the curve and the intersection points would look as in the figure below



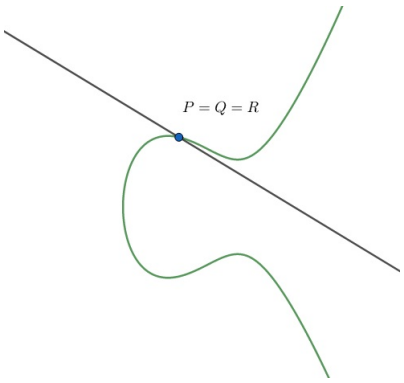
where every point has the intersection multiplicity 1 when the line and the curve intersects.

If we take the case $P = Q$, it would only occur exactly when G is the tangent to E at P according to definition 5.2. Because we have three points there will be some illustrations of how the elliptic curve looks with different intersection points depending on which points coincide.



In the case where two of the points coincide and one is distinct, results in a line intersecting the curve at only two points in the affine chart where the intersection multiplicity is either 1 or 2.

The third case when $P = Q = R$ only occurs when G is a flex point of the tangent at P since the intersection multiplicity would be 3.



Theorem 6.4. *Let C be a smooth cubic and let P, Q, R be points on C that are not necessarily distinct*

1. *R will be the third intersection of the line PQ if and only if there is a line l that intersects C at P, Q, R listed by multiplicity*
2. *If R is the third point of intersection of the line PQ, then Q will be the third intersection of the line PR, and R is the third point if intersection to the line PQ.*

If l is the line PQ whether or not P and Q are distinct ($P \neq Q, P = Q$). Since l intersects C at P, Q, R counting multiplicity, R will be the third point of intersection of the line with C.

Corollary 6.5. *All vertical lines will have its slope at infinity and therefore intersect the point at infinity.*

For this corollary we have two different proves, one mathematical and one graphical. Note that a vertical line is of the form $x = \lambda$ where x is the coordinate for every point on the line, and λ is where they line crosses the x-axis.

Proof. Since we are in the projective plane we will first homogenize the line such that we have

$$x_1 = \lambda x_0.$$

If we introduce another line that intersects the x-axis at a different point and put the two lines in an equation system

$$\begin{cases} x_1 = \lambda x_0 \\ x_1 = \mu x_0 \end{cases} \qquad \text{where } \lambda \neq \mu$$

and rearrange so that we have

$$\begin{cases} x_1 - \lambda x_0 = 0 \\ x_1 - \mu x_0 = 0. \end{cases}$$

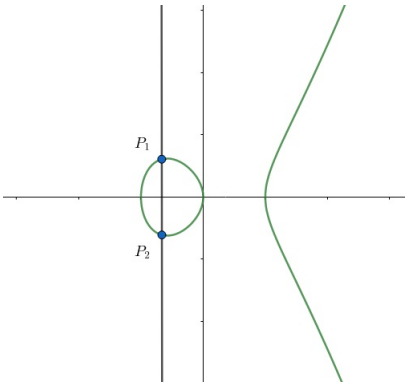
After performing a substitution (which can be done on either equation) we will receive the expression

$$x_0(\mu - \lambda) = 0.$$

Because $\lambda \neq \mu$ they cannot become zero and thus x_0 has has to be zero in order to satisfy the expression. Since λX_0 is the homogenization of x_1 we will have that it also takes on the value zero. This result in $x_2 \neq 0$ giving us the homogeneous coordinate $[0, 0, 1]$ that is the only solution different from zero, which is also the point at infinity. Thus, all vertical lines intersect at infinity.

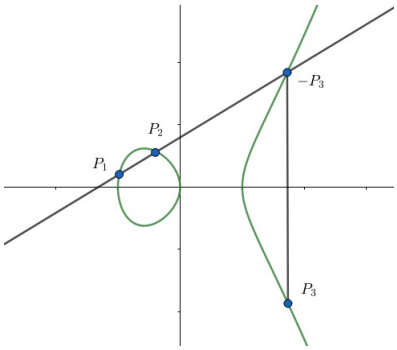
□

Proof. (Graphical) Consider the figure bellow

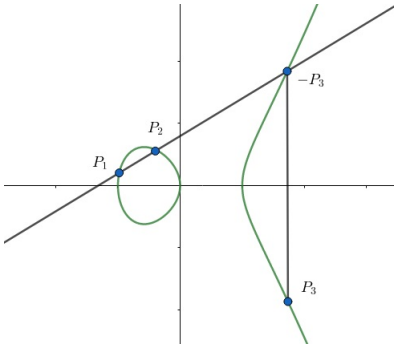


the curve has an ever increasing slope after a point of inflection, the slope will then also become infinite and thus intersect at infinity. Therefore the line P_1 to P_2 will intersect at infinity as well. □

If we wanted to perform addition of points on an elliptic curve in the case where we have two distinct points, P_1 and P_2, we first need to find the line between the two points. After finding the line we can find the third point of intersection. Lastly, we can reflect the third point of intersection to get the point P_3.



If we want to perform addition of points where the two point are not distinct $P_1 = P_2$, we will be adding a point to itself. In this case we would need to find tangent line instead, since it would have the intersection multiplicity two at the given point. With the tangent line we will then be able to find the third point of intersection. Finally, all we have left is to reflect the third point of intersection to find our desired point P_3.



To add points on an elliptic curve between two distinct points, $P_1 \neq P_2$, with the coordinates

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2)$$

we have to find the slope of the line, which we assign as λ.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

if we rearrange the equation we will get

$$y_2 - y_1 = \lambda(x_2 - x_1)$$

The slope will then be the intercept form of the line

$$y_2 = \lambda x_2 - \lambda x_1 + y_1$$

If we then introduce and define the variable β as $\beta = y_1 - \lambda x_1$ we will have

$$y_2 = \lambda x_2 + \beta$$

After defining the line, we want to find the coordinates for our third point of intersection $P_3 = (x_3, y_3)$. Which we are able to do by taking the line and changing it to fit the form of a curve by squaring the equation

$$y^2 = (\lambda x_2 + \beta)^2$$

now we can substitute our expression for y^2 in the equation of an elliptic curve

$$(\lambda x_2 + \beta)^2 = x^3 + ax + b.$$

After distributing and rearranging the equation above we will have the following polynomial

$$x^3 - \lambda^2 x^2 - 2\lambda x\beta - \beta^2$$

where $x_1, x_2, x_3 \in \mathbb{P}$ are the roots. Because the polynomial has the coefficient of x^2, which is the opposite sum of the roots. In other words $(x_1 + x_2 + x_3) = \lambda^2$. If we then rearrange the expression we will receive the equation for x_3:

$$x_3 = \lambda^2 - x_1 - x_2$$

If we want to find y_3, we can plug in the expression for x_3 in the equation of the original line and the reflect it (we multiply by (-1)). We will then have the expression for y_3

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

If we instead wanted to add points when the two points are equal to each other, $P = Q$, we would have to find the slope of the tangent line. We can find the slope by using the implicit function derivative on the elliptic curve which gives the slope.

$$dy2y = dx(3x^2 + 2ax + b)$$

After rearranging the equation and denoting the derivative as λ we will be given the equation of the slope as

$$\lambda = \frac{3x^2 + 2ax + b}{2y}.$$

We can use the equation from when we had two distinct point, but since the points are the same we only need to put the points $P_1 + P_2$ as $2P$ and similarly with their coordinates. We will then have the equation

$$x_3 = \lambda^2 - 2x_1$$

The y_3 coordinate is calculated the same way as for two distinct points.

By reflecting we take a point on a curve and try adding infinity, which we denote as O, to that point, and eventually receive a vertical line between that point and infinity. Then the third point of intersection will be the reflection of the original point.

When reflecting a reflection you will get back the original point.

$$P + O = P$$

thus making infinity the identity for point addition and our assumption of having one is correct.

Since we have identity, we should also have inverses. If we take point P_1 and reflect it, giving us point P_2, and then reflect that point. It would result in giving us infinity and thus making the reflection the points inverse. To conclude, the reflection of a point is its inverse.

So, if $P_1 = (x, y)$ and $P_2 = (x, -y)$ we will have

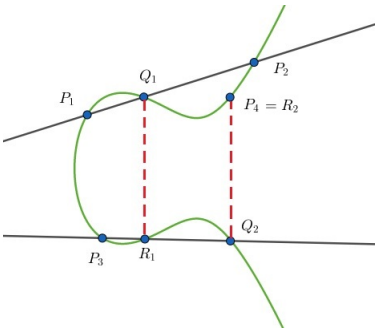
$$P_1 + P_2 = (x, y) + (x, -y) = (x, 0) = O.$$

From this we can draw the relation that a point added with its inverse will equal to the identity element.

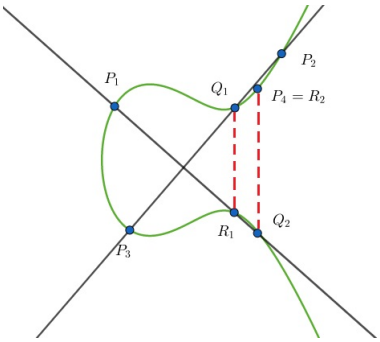
Since we are working with addition we need to prove its associativity. If we have the three points

$$(P_1 + P_2) + P_3 = P_4$$

where we first add P_1 to P_2 we will get a third point of intersection between the points, Q_1. If we then reflect Q_1, and call that point R_1, then add P_3 to the resulting point of reflection, we will receive a third point of intersection which we label Q_2. Lastly, if we reflect that point, we will receive our P_4, which is equal to R_2 as the second reflection point, as in the figure below.



If we take the same three points and start by adding P_2 to P_3 we will have a third point of intersection between the two points labeled as Q_1, after reflecting that point, we will get R_1. If we then add P_1 to R_1, we will have Q_2 as our third point of intersection of that line, and if we then reflect it we will receive the point R_2 which is equal to the point P_4, as shown in the figure below.



This seems to tell us that associativity holds, i.e.

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).$$

With these properties in mind, the curve E under point addition has an abelian group strucutre where the identity element is infinity, has inverses which are the reflections of points, and is also associative and commutative.

Example 6.6. If we wanted to check whether or not the curve $y^2 = x^3 + 8$ is elliptic, and if it is, find the second and third point of intersection. The point given to us is $(2, 4)$.

We already know that the curve is of degree three, which partially fulfills definition 6.1. Lastly, we need to check whether the curve is elliptic which we can do by checking if the

curve is smooth. We do that by taking the partial derivative and plugging in the coordinate to see whether or not the point is equal to zero:

$$\frac{\partial f}{\partial y} = 2y \text{ plug in the coordinate } = 8$$

and

$$\frac{\partial f}{\partial x} = 3x^2 \text{ plug in the coordinate } = 12.$$

Because the derivative is non-zero we can conclude that the curve is smooth and therefore an elliptic curve.

Due to the fact that we were only given one point we can safely assume that the second point of intersection will be given if we add the point on itself. Then we can utilize the equation above for point addition. We will start by finding the slope

$$\lambda = \frac{3(2)^2 + 2(0) + 0}{2(4)} = \frac{3}{2}$$

where a, b, c are zero since their terms are zero in the derivative. After finding the slope we can plug in the value to the equation for finding the x coordinate

$$x_3 = \left(\frac{3}{2}\right)^2 - 2(2) = \frac{9}{4} - 4 = \frac{-7}{4}.$$

Now we are able to find y_3 by putting in the values in the equation

$$y_3 = \lambda(x_1 - x_3) - y_1 = \left(\frac{3}{2}\right)\left(2 - \left(\frac{-7}{4}\right)\right) - 4 = \frac{13}{8}.$$

We have now found the second point of intersection, $P_2 = (\frac{-7}{4}, \frac{13}{8})$.

Next we want to find the third point of intersection. Because we have two distinct points now, we can utilize the equations for distinct points. We start first by finding the slope of the line between P_1 and P_2

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{4 - \frac{13}{8}}{2 - \frac{-7}{4}} = \frac{19}{30}.$$

After finding the slope we can find the x-coordinate for the third point of intersection

$$x_4 = \lambda^2 - x_1 - x_2 = \left(\frac{19}{30}\right)^2 - 2 - \left(\frac{-7}{4}\right) = \frac{34}{225}.$$

Now we can find the y-coordinate by putting in the values in the equation

$$y_4 = \lambda(x_1 - x_3) - y_1 = \left(\frac{19}{30}\right)\left(2 - \frac{34}{225}\right) - 4 = \frac{-9548}{3375}.$$

Lastly we need to check if the coordinates for our point of intersection satisfy the equation of the curve. For P_1 we see that

$$(4)^2 = (2)^3 + 8$$

which satisfies the equation so that $P_1 \in C$. For P_2 we can see that

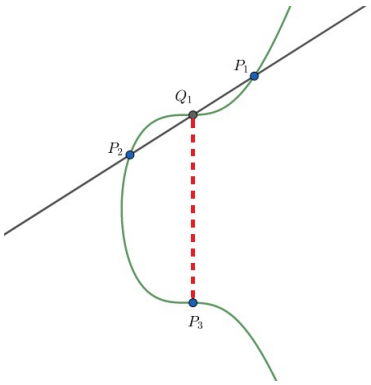
$$\left(\frac{13}{8}\right)^2 = \left(\frac{-7}{4}\right)^3 + 8$$

that also satisfies the equation, and $P_2 \in C$. For our last point P_3 we can see

$$\left(\frac{-9548}{3375}\right)^2 = \left(\frac{34}{225}\right)^3 + 8$$

that also satisfies the equation, and we have that $P_3 \in$.

To conclude, these points are our three points of intersection on the given curve since they satisfy the equation. We had the given point P_1 and added the point on itself, giving us P_2. Then we performed a second point addition that gave us Q_1 as the third point of intersection on the line P_1P_2, and after reflecting Q_3 we received our third point of intersection on the curve P_3.



References

Bix, Robert. *Conics And Cubics A Concrete Introduction To Algebraic Curves*. 2nd ed., Springer, 2006, https://link-springer-com.ezp.sub.su.se/content/pdf/10.1007

Gathmann, Andreas. Plane Algebraic Curves. 2018, https://www.mathematik.uni-kl.de/ gathmann/class/curves-2018/curves-2018.pdf. Accessed 13 May 2019.

Hulst, R.P. A Proof Of Bezout's Theorem Using The Euclidean Algorithm. 2011, https://www.math.leidenuniv.nl/scripties/HulstBach.pdf. Accessed 15 May 2019.

Kunz, Ernst. *Introduction To Plane Algebraic Curves*. 1st ed., Springer, 2005, https://link-springer-com.ezp.sub.su.se/. Accessed 11 May 2019.

Tao, Alex. Projective Geometry. 2008, https://www.ucl.ac.uk/ ucahmki/alex1.pdf. Accessed 11 May 2019.